Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Baptista Parra, 575
Praia do Suá - Vitória - ES
CEP 29052-123
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

| NSI-008 | V2.0 - AGO 2022 | SEGURANÇA DA INFORMAÇÃO |
|---|---|---|

# Cópia de Segurança e Restauração dos Arquivos Digitais do Tribunal Regional Eleitoral do Espírito Santo.

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Portaria DG/TSE 444/2021 - Instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitora

Normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

CIS Controls V.8

Palavras Chave: segurança, norma, backup, restore | 11 páginas

## 1. Prefácio

A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

## 2. Definições

Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG/TSE 444/2021, além dos seguintes:

- **arquivos digitais corporativos:** conjunto de sistemas, serviços e dados em suporte digital necessários à manutenção das atividades do Tribunal.
- **agente responsável:** área técnica gestora de um ambiente tecnológico (sistema, serviço, equipamento servidor etc) que deve ser mantido com cópia de segurança.
- ***backup* ou cópia de segurança:** conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação.

- ***backup* completo:** modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *backu.*

- ***backup* diferencial:** modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado.

- ***backup* incremental:** modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de qualquer modalidade efetuado.

- **criticidade:** grau de importância dos dados para a continuidade das atividades e serviços da organização.

- **descarte:** eliminação correta dos dados, unidades de armazenamento e acervos digitais.

- **restauração ou *restore*:** processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de *backup*.

- **retenção:** período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

- **janela de *backup*:** período de tempo durante o qual cópias de segurança, sob execução agendada ou manual, poderão ser executadas.

- **rotina de *backup*:** procedimento utilizado para se realizar um *backup*.

- ***unidade de armazenamento de backup:*** dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais.

## 3. Objetivo

Estabelecer a política de cópia de segurança (*backup*) e de restauração (*restore*) dos arquivos digitais do Tribunal Regional Eleitoral do Espírito Santo, instituindo diretrizes, responsabilidades e competências que visam garantir a segurança, a integridade e a disponibilidade dos dados custodiados pelo Tribunal Regional Eleitoral.

## 4. Abrangência

4.1. Esta norma se aplica aos arquivos digitais corporativos armazenados na infraestrutura tecnológica de equipamentos servidores físicos e virtuais que integram a rede local do Tribunal Regional Eleitoral do Espírito Santo.

4.2. Esta norma não se aplica aos arquivos digitais corporativos armazenados localmente pelos usuários em estações de trabalho corporativas (microcomputadores, notebooks, dispositivos móveis, tablets etc) e em dispositivos pessoais.

4.3. Esta norma não se aplica aos arquivos digitais corporativos armazenados em serviços de nuvem de terceiros, sejam eles de uso particular ou contratados pelo TRE-ES.

4.3.1. A salvaguarda e a recuperação dos arquivos digitais corporativos custodiados por outras entidades, públicas ou privadas, e utilizados pelo TRE-ES, deverão estar estabelecidas em cláusulas contratuais.

## 5. Das disposições gerais

5.1. Devem ser realizadas cópias de segurança dos arquivos digitais corporativos relevantes de forma regular e automática, com obrigatoriedade de realização de cópia de segurança integral dos sistemas críticos do Tribunal.

5.2. As cópias de segurança devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

5.3. As soluções utilizadas para a realização das rotinas de cópia de segurança devem cumprir os requisitos necessários para preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade das informações.

5.3.1. Os arquivos de cópias de segurança devem ser armazenados de forma criptografada (*data at rest*), considerando as normas vigentes.

5.3.2. Devem ser implementados controles criptográficos para o tráfego dos arquivos de cópias de segurança na rede do TRE-ES ou na Internet (*data in transit*).

5.4. A infraestrutura utilizada para a realização das rotinas de cópia de segurança não pode utilizar os mesmos controladores de domínio do restante da infraestrutura nem os dos usuários comuns, devendo ainda, ficar em rede totalmente apartada e protegida por firewall.

## 6. Das rotinas de cópia de segurança e de restauração de arquivos digitais

6.1. O planejamento das cópias de segurança deve ser orientado para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

6.2. As rotinas de cópia de segurança devem ser executadas, sempre que possível, sem a paralisação dos sistemas, serviços, equipamentos servidores e bases de dados.

6.3. As rotinas de cópia de segurança devem ser organizadas em janelas de execução que não comprometam o regular funcionamento dos serviços de tecnologia da informação, preferencialmente em períodos de baixa utilização dos recursos computacionais e fora do horário de expediente ordinário das unidades da Secretaria do Tribunal.

6.4. As cópias de segurança devem ser testadas regularmente por meio de testes de recuperação/restauração (*restore*), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento).

6.5. Os registros de atividades (*logs*) das rotinas de cópia de segurança e de restauração de dados também devem ser mantidos em cópias de segurança, com retenção de acordo com o estabelecido na norma de gestão de *logs* do Tribunal.

6.6. Os parâmetros referentes às rotinas regulares de cópia de segurança e de restauração de arquivos digitais deverão ser detalhados em um Plano de Gerenciamento de Cópias de Segurança e de Restauração de Arquivos Digitais, a ser elaborado e mantido pela área técnica responsável pela gestão das cópias de segurança.

## 7. Do Plano de Gerenciamento de Cópias de Segurança e de Restauração de Arquivos Digitais

7.1. O Plano deve refletir os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos, alinhando-se ao Plano de Continuidade de Negócios do Tribunal e à Política de Segurança da Informação da Justiça Eleitoral.

7.2. São parâmetros mínimos exigidos no Plano:

7.2.1. Escopo (dados a serem salvaguardados/restaurados);

7.2.2. Agente responsável pelos dados;

7.2.3. Tipo (completo/total, incremental e diferencial);

7.2.4. Frequência (diária, semanal, mensal e anual);

7.2.5. Tempo de retenção;

7.2.6. Unidade de armazenamento;

7.2.7. Janela de *backup*;

7.2.8. Local de armazenamento das mídias;

7.2.9. Tempo máximo para a restauração do *backup*;

7.2.10. Periodicidade do teste regular de restauração do *backup.*

7.3. As rotinas de cópia de segurança e de restauração de dados para fins de cumprimento do Plano devem ser mantidas pela área técnica responsável pela gestão das cópias de segurança.

7.4. Os procedimentos de execução dos testes regulares de restauração do *backup* para fins de cumprimento do Plano devem ser mantidos pelos agentes responsáveis.

7.5. O Plano deve descrever os requisitos específicos de segurança da informação aplicáveis às cópias de segurança, detalhando, por exemplo: o controle de acesso lógico, a segurança do local de armazenamento e a existência de cópia em local remoto seguro diferente do original, entre outros.

7.6. A documentação do Plano deve ser armazenada em local seguro e com acesso restrito à área técnica responsável pela gestão das cópias de segurança e pelos Agentes Responsáveis.

7.6.1. As partes interessadas devem ser comunicadas em relação aos aspectos que impactam no negócio, em especial: escopo, tipo, tempo de retenção e tempo máximo para restauração do *backup*.

7.7. Caberá à Comissão de Segurança da Informação, em 1ª instância, e à Administração, em 2ª instância, a aprovação do Plano.

## 8. Dos tipos, frequência e retenção dos dados de *backups*

8.1. Os *backups* devem ser realizados observando-se o tipo, a frequência e o tempo de retenção definidos no Plano de Gerenciamento de Cópias de Segurança e de Restauração de Arquivos Digitais.

8.2. Os *backups* dos sistemas devem ser realizados utilizando-se os seguintes tipos:

8.2.1. completo/total;

8.2.2. incremental; ou

8.2.3. diferencial.

8.3. Os *backups* dos sistemas devem ser realizados utilizando-se as seguintes frequências temporais:

8.3.1. diária;

8.3.2. semanal;

8.3.3. mensal; ou

8.3.4. anual;

8.4. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

## 9. Da definição dos ambientes mantidos com cópia de segurança e dos Agentes Responsáveis

9.1. São ambientes mantidos com cópia de segurança:

9.1.1. Os serviços e sistemas tecnológicos corporativos, sendo agente responsável a área técnica mantenedora do respectivo serviço ou sistema.

9.1.2. As bases de dados corporativas, sendo agente responsável a área técnica mantenedora do sistema gerenciador de banco de dados.

9.1.3. Os equipamentos servidores físicos e virtuais e suas configurações, que não estejam diretamente associados a um sistema ou serviço específico, sendo agente responsável a área técnica mantenedora do núcleo de infraestrutura.

9.1.4. Os arquivos corporativos de usuários que, ao serem armazenados nos equipamentos servidores destinados a este fim, são automaticamente inseridos nas rotinas de cópia de segurança.

9.1.5. Arquivos de registro de atividades (logs), observando-se política de retenção específica, caso haja.

## 10. Dos testes regulares de restauração do *backup*

10.1. Os *backups* devem ser testados periodicamente, ao menos mensalmente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

10.2. Os testes de restauração dos *backups* devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

## 11. Das restaurações sob demanda

11.1. As solicitações de restauração de dados devem ser realizadas formalmente por meio de ferramenta de abertura de chamados técnicos.

11.2. No caso de solicitação de recuperação de arquivos de usuários, os pedidos deverão conter o nome dos arquivos, as pastas que deverão ser recuperadas e a data dos arquivos que se pretende recuperar.

11.3. No caso de restauração de sistemas, serviços, servidores ou base de dados, o agente responsável deverá fornecer todas as informações capazes de identificar unicamente o item que deve ser restaurado.

## 12. Das unidades de armazenamento de *backups*

12.1. A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados deverá atender às seguintes características dos dados resguardados:

12.1.1. a criticidade;

12.1.2. o tempo de retenção;

12.1.3. a probabilidade de necessidade de restauração;

12.1.4. o tempo esperado para restauração;

12.1.5. o custo de aquisição da unidade de armazenamento de *backup*;

12.1.6. a vida útil da unidade de armazenamento de *backup; e*

12.1.7. a disponibilidade de recursos.

12.2. O *backup*, de acordo com sua criticidade, deve ser provido em 2 (duas) mídias distintas, com conteúdo idêntico, para armazenamento em 2 (dois) locais diferentes, observado o seguinte:

12.2.1. uma cópia de segurança deve ser armazenada de forma a permitir sua rápida localização e recuperação;

12.2.2. outra cópia de segurança deve ser armazenada em local distinto da cópia principal;

12.2.3. ao menos uma cópia de segurança deve ser armazenada em uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

12.3. Os locais de armazenamento das mídias da cópia de segurança devem ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

12.3.1. O acesso ao local deve ser restrito e monitorado;

12.3.2. O acesso ao local deve ser registrado em logs contendo minimamente a identificação do usuário e informações de data e hora de entrada e saída;

12.3.3. O local deve possuir controles de prevenção, detecção e combate a incêndio.

12.4. A cópia de segurança referida no **item 12.2.2** pode ser armazenada em serviços de nuvem, desde que seja criptografada e gerenciada pela mesma solução de *backup*, observando-se, ainda, os cuidados de gerenciamento de acessos privilegiados e de bloqueio de redes de acesso.

12.5. Deverá ser identificada a viabilidade de utilização de diferentes tecnologias na realização dos *backups*, propondo a melhor solução para cada caso.

12.6. Poderão ser utilizadas técnicas de compressão de dados, respeitando-se o tempo máximo de restauração de dados previsto no Plano.

## 13. Do descarte e da substituição da cópia de segurança

13.1. O descarte e a substituição da mídia utilizada para geração da cópia de segurança devem respeitar o disposto na norma complementar específica da Política de Segurança da Informação.

13.2. Nos casos de substituição da solução de *backup* (*hardware* ou *software*), as informações contidas nas mídias da antiga solução devem ser transferidas, em sua totalidade, para mídias compatíveis com a nova solução.

13.2.1. A solução de *backup* obsoleta somente poderá ser desativada após a certificação de que todas as informações foram transferidas para a nova solução implementada.

13.3. Quando da necessidade de descarte de unidades de armazenamento de *backups*, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

## 14. Das responsabilidades

### 14.1. Da Comissão de Segurança da Informação

14.1.1. Aprovar em 1ª instância o “Plano de Gerenciamento de Cópias de Segurança e de Restauração de Arquivos Digitais”.

14.1.2. Deliberar sobre as ações a serem adotadas em caso de desrespeito aos termos desta norma.

14.1.3. Manter atualizados os dispositivos desta norma.

### 14.2. Da área técnica responsável pela gestão das cópias de segurança

14.2.1. Planejar os recursos necessários para cumprimento de todas as obrigações dispostas nesta norma.

14.2.2. Elaborar e propor o Plano de Gerenciamento de Cópias de Segurança e de Restauração de Arquivos Digitais.

14.2.3. Cumprir o Plano de Gerenciamento de Cópias de Segurança e de Restauração de Arquivos Digitais.

14.2.4. Gerenciar e manter atualizada a solução de *backup* do Tribunal, com adoção de tecnologias especializadas.

14.2.5. Criar e gerir as rotinas de cópias de segurança e de restauração:

14.2.5.1. Efetuar medidas preventivas para evitar falhas;

14.2.5.2. Gerenciar mensagens e registros de auditoria (logs);

14.2.5.3. Verificar periodicamente os eventos gerados, tomando as providências necessárias para remediação de eventuais falhas.

14.2.5.4. Comunicar aos Agentes Responsáveis a ocorrência de falhas.

14.2.6. Providenciar a execução dos testes regulares de restauração do *backup*, mediante solicitação dos Agentes Responsáveis.

14.2.7. Restaurar ou recuperar as cópias de segurança em caso de necessidade.

14.2.8. Gerenciar mídias.

14.2.9. No âmbito do TRE/ES, o papel de gestão caberá a Seção responsável pelo Gestão de Infraestrutura e Redes vinculado à Coordenadoria de Infraestrutura Tecnológica e Segurança Cibernética.

**14.3. Dos agentes responsáveis por ambientes mantidos com cópia de segurança**

14.3.1. Pedir a inclusão, a alteração ou a remoção de arquivos digitais sob sua responsabilidade nas rotinas de cópia de segurança.

14.3.2. Indicar todos os diretórios, arquivos de configuração, equipamentos servidores, arquivos de registro de atividades (logs), etc., que devem ser incluídos nas rotinas de cópia de segurança.

14.3.3. Definir os procedimentos para realização dos testes regulares de restauração dos arquivos digitais sob sua responsabilidade.

14.3.4. Solicitar a execução das rotinas dos testes regulares de restauração dos arquivos digitais sob sua responsabilidade.

14.3.5. Avaliar e atestar o resultado dos testes regulares de restauração dos arquivos digitais sob sua responsabilidade, mantendo os registros arquivados para fins de consulta, auditoria e investigação de ilícitos cibernéticos.

**14.4. Da área técnica responsável pela segurança cibernética**

14.4.1. Propor soluções para aprimorar os processos e procedimentos técnicos relacionados à cópia de segurança e à restauração de dados, visando aumentar a segurança dos dados;

14.4.2. Verificar junto às Unidades Técnicas o regular cumprimento dos dispositivos vigentes relacionados à cópia de segurança e à restauração de arquivos digitais.

14.4.3. No âmbito do TRE/ES, o papel caberá ao Núcleo de Segurança Cibernética vinculado à Coordenadoria de Infraestrutura Tecnológica e Segurança Cibernética.

**14.5. Dos usuários**

14.5.1. Armazenar os arquivos digitais corporativos sob sua responsabilidade nos equipamentos servidores devidamente destinados a este fim.

14.5.2. Não armazenar arquivos digitais de caráter particular nos equipamentos servidores objeto de cópia de segurança.

14.5.3. Tomar conhecimento dos períodos de retenção das cópias de segurança relacionadas aos arquivos digitais sob sua responsabilidade.

14.5.4. Solicitar imediatamente a restauração de dados eventualmente apagados ou perdidos, por meio dos canais apropriados e prestando as informações necessárias para a recuperação.

## 15. Das disposições finais

15.1. Os casos omissos nesta norma deverão ser resolvidos pela Comissão de Segurança da Informação.

15.2. A implementação desta norma iniciará imediatamente e deverá estar concluída no prazo de 12 (doze) meses a contar da data da sua publicação.